Loyola Consumer Law Review

Volume 34
Issue 3 *Symposium Issue 2022*

Article 2

2022

Exploring the Role of Technology in Consumer Law Enforcement

Liz Coll
Connected Consumers

Christine Riefa
University of Reading

EXPLORING THE ROLE OF TECHNOLOGY IN CONSUMER LAW ENFORCEMENT

Liz Coll, Connected Consumers
Prof. Christine Riefa, University of Reading

I. INTRODUCTION

Almost two thirds of the global population have access to the internet in some form[1], and by 2020, 27% of people had shopped online.[2] Major investments in infrastructure around the world are fuelling a move towards even more use of the Internet as the backdrop to consumers' lives. But consumer laws which, by and large, were devised prior to the advent of the Internet, have struggled to prevent or offer reparation for the harm suffered by consumers online. While many laws protecting consumers have slowly adapted to cope with the new challenges brought by digitalization, the way the enforcement of those laws takes place has not evolved at the same pace.

Enforcement is a distinct component of consumer protection. It is less visible and receives less scrutiny than policy setting, legal drafting and regulatory approaches and principles. It is, however, instrumental in ensuring consumers are adequately protected. Yet, both public and private consumer enforcement are limited in their ability to protect consumers and have been notoriously difficult to achieve[3]. Consumer awareness of their rights is generally low and damages and redress can only be sought after the harm has taken place, with the onus on

---

[1] ITU statistics for 2021 estimate that approximately 4.9 billion people or 63 per cent of the world's population are using the Internet in 2021, representing an increase of 17 per cent since 2019 https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[2] UNCTAD, B2C E-commerce Index 2020, UNCTAD Technical Notes on ICT for Development No17

[3] Riefa, C (2020) Coronavirus as a Catalyst to Transform Consumer Policy and Enforcement. *Journal of Consumer Policy 43 (3), 451-461* https://dx.doi.org/10.1007/s10603-020-09462-0

individuals to take action. This requires time and resources to navigate enforcement mechanisms such as court claims or ADR where available. Public enforcement is equally insufficient as very limited resources mean only a fraction of problems are prioritised, leaving some harms unchecked in the marketplace.

Digital technology is often branded as a tool for the empowerment of consumers on the demand side of the market. Yet so far enforcers have not embraced technology to enable the monitoring and sanctioning of the supply side as readily as industry have embraced it to deliver new services. As Schrepel observes '*while there are passionate discussions about the practices implemented by digital players, the use of technological tools to address them is very little debated*'[4]

The use of technology in enforcement is only nascent. However, a number of consumer enforcement authorities (notably FTC in the USA and CMA in the UK) are making changes to account for and harness technology in their enforcement practice with other authorities likely to follow.

In this article we take stock of the use of technological approaches to consumer law enforcement and compliance as well as review existing technologies which identify, monitor and redress detriment. While the goal is not to recommend the adoption of any particular technological strategy, the hope is that this article will assist in understanding both the value and the potential risks of the use of technology in enforcement. This article starts by reflecting on why technology ought to play a role in consumer law enforcement. It then moves to exploring the opportunities technology could offers, before reflecting on the potential pitfalls.

II. WHY SHOULD TECHNOLOGY PLAY A ROLE IN ENFORCEMENT?

One of the first question to address is why should technology play a role in enforcement? The answer stems directly from the type of harms enforcement agencies must grapple with.

Technology seems to unfortunately require yet more technology to be effectively addressed as it appears quasi-impossible to curb some of

---

[4] Schrepel, T, Computational Antitrust: An Introduction and Research Agenda (January 15, 2021). Stanford Computational Antitrust (Vol. 1) 2021. https://ssrn.com/abstract=3766960

the harms experienced by consumers without technological back up. These include for example: Harms resulting from the legitimisation of rights-infringing practices, which have been directly exacerbated by the use of technology. One typical example is the mass use of unfair contract terms. Online consumers enter into a large number of contracts, often instantaneously.[5] They are unable to read and digest them all.

Contractual clauses that are tilted in favour of businesses are thus prevalent in the terms of online services despite legislation designed to prevent them in certain regions of the world, notably the EU.[6] These include terms that grant the online service provider a right to: unilaterally change the terms of service or the service itself; unilaterally terminate the contract, terms that exclude or limit liability, international jurisdiction clauses and choice of law clauses.[7] It is extremely difficult for a human being to monitor changes to terms and detect unfair ones that may require intervention. Technology can offer some solution and make enforcement more effective. Harm can also derive from the intermediary platform model which limits the information available to consumers about pricing, availability or quality and provenance leading them to make sub-optimal choices. These practices are effectively designed into the structure and performance of the platform via algorithms, meaning that an understanding of the technology driving their operation is essential to evidence their existence and understand where intervention may be required.

The reasons for exploring the use of technology in consumer enforcement are also relevant in the context of the salient problem of resource asymmetry. This is because the technical knowledge, legal expertise and financial resources available to large companies who may come under scrutiny by public enforcers can outweigh that of national regulators. As businesses are now rolling out technological solutions in their operation, enforcers need to 'tool up' in order to effectively continue to meet their legal obligations.

The current situation has shown that when faced with enforcement

---

[5] Micklitz, HW, Pałka, P. and Panagis, Y (2017) The Empire Strikes Back: Digital Control of Unfair Terms of Online Services. *Journal of Consumer Policy* 40, 367–388 https://doi.org/10.1007/s10603-017-9353-0

[6] Micklitz, HW et al (2017)

[7] Loos, Marco and Luzak, Joanna Aleksandra (2015) Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers. *Journal of Consumer Policy 2016/1*, p. 63-90, http://dx.doi.org/10.2139/ssrn.2546859

action, companies can often well afford to contest numerous claims across multiple jurisdictions over a long period of time. Even when decisions go against them, the appeal process can span years and the implementation of changes can be comfortably delayed. This may lead to decisions being disregarded by Big Tech companies and fines factored in as a cost of doing business.[8] This can then undermine confidence of consumers in the public enforcement actions and results in consumers becoming disengaged and perhaps not reporting bad practice.

One further important reason to explore the use of technology in enforcement is the fact that some scholars have convincingly demonstrated that all consumers are in fact made vulnerable by the structure of digital markets[9] notably because of the use of technologies that remove consumers' ability to make decisions or impair the decision-making process[10] alongside the reliance on huge platform conglomerates to access essential services and consumer functions.

Digital vulnerability may be even more worrying for it is not only contemporary to decision making in the here and now, but also extends into the future. In the absence of regulatory intervention, the risk is that consumers may also be made vulnerable to things that have not yet materialised – for example the impact of mass data collection over several years on large populations leaves companies with vast swathes of insights about collective and individual behaviours.[11] There is therefore some urgency in finding adequate tools to control the operation of digital markets and prevent as well as repair the harm experienced by consumers.

---

[8] See for example, Netherlands Authority for Consumers and Markets (ACM) (21 January 2022) *Apple fails to satisfy requirements set by ACM.* Press Release. Retrieved from https://www.acm.nl/en/publications/apple-fails-satisfy-requirements-set-acm

[9] See notably Riefa, Protecting vulnerable consumers in the digital single market, *European Review of Business Law* Vol. 3, issue 4, August 2022 and Micklitz, Helberger et al., (2021) EU Consumer Protection 2.0: Structural asymmetries in consumer markets, https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf

[10] Riefa, 2020

[11] Micklitz, Helberger et al., 2021

III. WHAT COULD A TECHNOLOGICAL APPROACH TO ENFORCEMENT OF CONSUMER PROTECTION LOOK LIKE?

This leads us to reflecting on the how technological innovations help deliver enforcement activities at a speed and breadth that better matches online activities.

One important distinction to draw from the outset concerns the regulatory functions that need to be fulfilled and/or assisted by technology. To date, they have been classified according to the user or beneficiary of the technology. On the one hand, supervisory authorities have made use of Supervisory Technology (SupTech) to facilitate and enhance supervisory processes.[12] On the other, companies have used technology for the management of regulatory processes and to ensure compliance (RegTech).[13] It flows from there that technology servicing the needs of enforcement authority can be coined (Enf Tech). Currently, the literature does not tend to distinguish between the types of use for technology.[14] However, it is also helpful to consider not just the user of the technology, but how the technology is used indeed: Technology can implement the direct execution of an enforcement action such as a warning, takedown or sanction.[15] It can implement a remedy such as a refund or correction of service remotely and automatically.[16] In this regard, the use of the technology can also be deemed to class as 'Enforcement Technology' (or EnfTech) because it focusses on delivering a remedy.

EnfTech may require the collaboration of businesses and enforcement authority to take shape as enforcement is normally practiced *ex post*.

---

[12] For example, the Financial Intelligence Unit at the Bank of Italy explores huge data sets to measure anomalies in suspicious transaction reports. This is then used to classify the reports according to the type of money laundering scheme and track and sanction more easily.

[13] For example, systems that analyse regulations across multiple jurisdictions, extract rules, map them against organisations internal procedures and automatically alert relevant staff if new action needs to be put in place.

[14] See also Goanta Spanakis (2022) who distinguish between market surveillance and digital enforcement.

[15] For example, the automatic removal of harmful content or copyright infringing content by companies.

[16] For example, in the UK, where a passengers' booking and payment was linked to a specific train journey, an automatic refund is paid out in the case of a delay to that service

But EnfTech could find uses *ex ante*, ie before the damage to consumers is felt. For example, it is possible to envisage technology that is used to prevent infringements by reviewing product features, provenance and safety prior to them entering the market, or reviewing contractual terms prior to consumers entering into agreements. In those cases, while enforcement authorities may be able to survey market activity, they will often also need access to companies' data to be most effective.

Therefore, more generally, in this article EnfTech is conceptualised as the overall set of tools enforcers have at their disposal and which can encompass elements of SupTech, RegTech and forms of EnfTech focussed on sanctioning or preventing behaviours. EnfTech concerns not only monitoring or reporting but also the active application of preventative measures, remedies or sanctions that support consumer protection. Developing the ability to deliver direct execution of enforcement in national and cross-border settings will be critical in enhancing the functioning of consumer protection in future years.

Embedding technology in consumer protection enforcement could be well suited to challenges specific to digital consumer markets and interactions such as: analysing a high volume and high speed of transactions and complaints to identify patterns of bad practice; creating the digital identification of products and the ability to take-down harmful products and track and trace them to their source; and automatically executing remedies directly to consumers.

There is already many technological tools available servicing the many EnfTech functions that come within the current remit of consumer enforcement authorities and could be adapted to their needs. [17] Technology is already applied to enforce ex post. For example, the Alibaba Group has a monitoring tool to tackle online counterfeiting and piracy. It uses product identification modelling, image recognition, semantic recognition and product information databases to identify fake products and real-time interception systems to serve take-down notices. Further, through tracing the movement of funds and finance, it can identify counterfeiters and the factories producing the goods.[18]

---

[17] For more details, see Riefa et al., *Cross border enforcement of consumer law: looking to the future* (May 2022) available at www.crossborderenforcement.com

[18] World Intellectual Property Organisation (2018) The global digital enforcement of intellectual property. Retrieved from: https://www.wipo.int/wipo_magazine/en/2018/si/article_0005.html

Technology has been embedded in the enforcement of copyright breaches since the adoption of the Digital Millennium Copyright Act (DCMA) in 1998. Through algorithmic enforcement, online content platforms use automated search and takedown tools to remove material that breaches copyright. Copyright owners issue huge volumes of takedown requests to platform intermediaries via robots. The platforms use algorithms to filter, block, and disable access to allegedly infringing content automatically, with minimal or no human intervention.[19] In other consumer settings, this type of technology can help with, for example, detecting goods that have been identified as fake on online platform. Similar technology could be adopted in the context of unfair commercial practices for example, providing those clear legal interpretations can be offered to data coders.[20]

Perhaps the biggest value of EnfTech tools would be to reverse the current, unsatisfactory enforcement journey that consumers face: a consumer experiencing a harm, being able to relate it to a specific legal breach, gathering evidence of the harm, bringing it to an alternative dispute resolution system or to a court, or reporting it to a public authority in the hope of action being taken to remedy or prevent it. It is already possible to apply technological tools in an ex-ante enforcement set up by anticipating misconduct. The Monetary Authority of Singapore (MAS) uses existing reports of misconduct by financial adviser representatives working at insurers, banks, and financial advice firms to develop a series of predictive factors (such as previous work experience or misconduct history of the representative) for those most likely to selling unsuitable life insurance or investment products to consumers.[21] Companies also already use ex-ante tools notably in fraud identification. Payment platforms like PayPal have pioneered machine learning systems to identify fraud. Databases of legitimate and fraudulent credit card transaction information such as date, time, merchant, merchant location and price were used to train the algorithm

---

[19] Perel, M and Elkin-Koren, N (2016) Accountability in Algorithmic Copyright enforcement. Stanford Technology Law Review 473 http://dx.doi.org/10.2139/ssrn.2607910

[20] On this point, see Goanta, Spanakis (2022) 46.

[21] Case study featured in Appendix 1 of The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions: Market developments and financial stability implications (fsb.org)

to accurately predict frauds before they occur.[22]

Enforcement could also be transformed by the implementation of promising prototype projects such as:

- 'uTerms' a software that reads and highlights potentially unfair terms and automates the time-consuming processes of reading, reviewing and judging the likelihood of unfairness of clauses are particularly attractive. [23] They could be used by consumers to protect themselves and avoid those contracts, by businesses seeking compliance and enforcers alike. A stage further from this, we could envisage an auto-executed ('smart' style) contract cutting out the need for a third party to run the analysis of clauses and simply removing or remedying for unfair terms based on the legal framework the company is subject to.
- Stanford University's Computational antitrust project which envisages the use of automated legal reasoning during activities or when activities are planned, as opposed to ex-post. This is likened to a 'driving instructor' in the backseat, a non-punitive agent alerting a novice driver if they are about to break a traffic law and advising an alternative action. The punitive version of this would be an agent with the power to immediately alert the authorities of violations when the driver ignores the advice. The examples here involve individuals subject to criminal law but could be applied to companies. Indeed, this is the job many RegTech applications perform, altering prior to action where rules might be broken.
- We might easily then imagine the 'computerised police enforcer' able to notify authorities or consumers directly that a law has been broken and enabling the next stage of enforcement or redress. This might be automating an immediate refund to a consumers, or initiating a change to service terms and practice, or perhaps entering the consumer into an opt-in class action, or retaining their details when an opt-out class action is at the distribution stage. To improve visibility of such tools, we might imagine a notice similar to the regular reports from anti-

---

[22] HBS.edu Technology and Operations Management (2018) PayPal's Use of Machine Learning to Enhance Fraud Detection (and more). Retrieved from: https://digital.hbs.edu/platform-rctom/submission/paypals-use-of-machine-learning-to-enhance-fraud-detection-and-more/

[23] Micklitz et al., 2017

virus software providers which tell you how many attacks were spotted and prevented: '*X number of unfair contractual clauses were spotted today and were removed from agreements you entered into.*'

1. What are the potential pitfalls of the use of Enf Tech?

Technological solutions look promising, but they are not a panacea. They come with their own set of challenges. For large scale, regulator-led roll out of enforcement enabled by technology (including across borders), several factors must be considered. The list below is by no means exhaustive but ought to warn against the most salient problems that need to be addressed by enforcement authorities and to some extent policy makers as the roll out of tech tools will often also require the enactment of a new legislative framework enabling their use.[24]
Firstly, the quality of the data required by enforcement authorities. This could be from static data sets or live feeds of information on transactions and contracts. The quality and format of this data is critical for ensuring that activity can be monitored within and across borders. Financial regulatory authorities have begun to explore how to translate regulatory rules into machine-readable formats so that reporting and compliance can be more easily automated, but currently the absence of common standards is holding back developments. As well as data, systems must also be compatible with each other and able to communicate effectively within and across jurisdictions. The European Commission is developing a strategy on supervisory data which will involve standardisation and interoperability.[25] However, for consumer protection

---

[24] In the EU for example, the CPC Regulation 2019/2020, article 9(4)(g), gives market surveillance authorities powers to:
- remove content or restrict access to an online interface and order the display of consumer warnings on the said interface
- order a hosting service provider to remove, disable or restrict, access to an online interface
- order the deletion of a domain name before domain registries and allow competent authorities to register it.
Note also that the proposed EU AI Act plans to give surveillance authorities some powers to investigate compliance with the Act for high-risk systems already placed on the market (see section 5.2.6 of the proposal).

[25] European Commission, DG Financial Stability, Financial Services and Capital Markets Union (2021) Strategy on supervisory data in EU financial services. Retrieved from: Strategy on supervisory data in EU financial services | European Commission (europa.eu)

the situation may be different. In e-commerce for example, there is not a history of reporting requirements[26] and so making rules machine readable and data portable would start from a different point. A related point to note is that the over reliance on data which reflects existing structures and biases and exacerbates prevalent bias is well-recognised as a risk in AI systems.[27] The same risk arises in EnfTech, where for example, data on consumer complaints used to develop or train machine learning models is unlikely to represent the experiences of all consumers, particularly those who face particular disadvantages.

Secondly, there is emerging evidence companies are inclined to game the system by adapting their behaviour to avoid attention. There has been speculation that companies may increase the use of self-destructing encrypted data to make evidence for investigations difficult[28]. Research by Cao et al found that '*growing AI readership...motivates firms to prepare filings that are friendlier to machine parsing and processing. Firms avoid words that are perceived as negative by computational algorithms, as compared to those deemed negative only by dictionaries meant for human readers.*'[29] This may therefore mean that enforcers tooling up starts an arms race with businesses that enforcers may not be able to win, thus compounding the already existing asymmetry.

Thirdly, there is a possible danger that enforcers, for lack of in-house expertise or driven by economic efficiency, come to rely on already existing technologies. Goanta and Spanakis talk of public authorities remaining tech users rather than becoming tech makers, potentially leading to a privatisation of the public enforcement.[30] In private enforcement, the privatisation of the process has been highly criticised. ADR has come to largely replace courts in many countries and is not delivering well for consumers.

---

[26] There is also evidence that the recording of infringements is also vastly disjointed, notably concerning scams.

[27] The Council of Europe, 2021: Artificial intelligence, human rights, democracy, and the rule of law: a primer.

[28] Competition Bureau Canada (2020) Digital Enforcement Summit 2020. Retrieved from https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04563.html#panel3

[29] Cao, Sean S. and Jiang, Wei and Yang, Baozhong and Zhang, Alan L (2020*), How to Talk When a Machine is Listening: Corporate Disclosure in the Age of AI.* https://dx.doi.org/10.2139/ssrn.3683802.

[30] Goanta, Spanakis, Discussing the legitimacy of digital market surveillance (2022) Stanford Computational Antitrust vol II, p.54.

Finally, the development of technology-based supervision and enforcement solutions by authorities would require co-ordination and collaboration in ensuring that best practice is not just limited to one jurisdiction and to avoid costly duplication of development work. There is to date very little talk of developing a global approach although the 2019 OECD report[31] is worthy of notice in that it recommended fostering peer learning with regards to the successes and failures of SupTech uses.

IV. CONCLUSION

Huge potential lies in taking the best of technology and applying it to solving problems of technology with a reinvigorated approach to enforcement and supervision. Adapting existing systems to consumer protection is a viable proposition, but one that needs more research and exploration to enable it to grow in a positive way.

It is often a tempting option to apply technology to streamlining and efficiencies as opposed to more transformative means, however authorities must be wary of digitising a broken system. If enabling more effective use of enforcement technology for consumer protection is only focused on speeding up the current, flawed system it will be a missed opportunity. Instead, the move to the use of tech in consumer law enforcement could signal a shift in the way enforcement functions are thought about and executed. This in turn could go some way to addressing the lack of incentives to stick to the law, which impacts on competition, and give enforcement the visibility it needs to instil confidence in consumers that bad behaviour will be kept in check. This trend towards the use of technology in enforcement links well with already established academic work that signalled a clear shift for the approach towards what Willis has coined performance-based consumer law[32] [33] or Siciliani, Riefa, Gamper addressed as a need for fairness by

---

[31] OECD (2019), "Using digital technologies to improve the design and enforcement of public policies", OECD Digital Economy Papers, No. 274, OECD Publishing, Paris, https://dx.doi.org/10.1787/99b9ba70-en. Open DOI

[32] Willis, Lauren E., Performance-Based Remedies: Ordering Firms to Eradicate Their Own Fraud. 80 Law and Contemporary Problems 7-41 (2017), Loyola-LA Legal Studies Research Paper No. 2017-26. https://ssrn.com/abstract=3018168

[33] Willis, Lauren E., Performance-Based Consumer Law. 82 University of Chicago Law Review 1309 (2015), Loyola-LA Legal Studies Paper No. 2014-39, Available at SSRN: https://ssrn.com/abstract=2485667

design[34] in consumer markets. The ability to expect businesses to behave and if not, expect sanctioning could be furthered thanks to a technological approach to enforcement.

[34] Siciliani, P, Riefa, C, & Gamper, H. (2019). *Consumer Theories of Harm: An Economic Approach to Consumer Law Enforcement and Policy Making.*